Some cryptographic properties of near bent functions over finite fields

Prasanna Poojary
Department of Mathematics
Manipal institute of Technology
Manipal Academy of Higher Education
Manipal, Karnataka
India

P.K. Harikrishnan
Department of Mathematics
Manipal institute of Technology
Manipal Academy of Higher Education
Manipal, Karnataka
India

Vadiraja Bhatta G. R.*
Center for Cryptography
Manipal institute of Technology
Manipal Academy of Higher Education
Manipal, Karnataka
India
and
Department of Mathematics
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal, Karnataka
India
vadiraja.bhatta@manipal.edu

Abstract. We present a method for construction of near bent function with the help of Gold power functions. We have also investigated the cryptographical properties, i.e., non-linearity, correlation immunity, algebraic immunity and algebraic degree of these functions.

Keywords: boolean functions, near bent functions, trace, walsh coefficient, cryptography.

1. Introduction

In the modern days the communication between two individuals, or among groups of people, or social establishments requires high security of the message

∗. Corresponding author

or information. Boolean functions have been studied due to their cryptographic properties for the last two decades. These functions play a significant role in constructing components of symmetric ciphers. Boolean functions used in cryptographic applications provide security of a cipher against different kinds of attacks.

Nonlinearity of a Boolean function is an essential property and functions with high non-linearity have applications in cryptography. Shannon in [1] identified that confusion and diffusion are the essential technique for performing security. Confusion could be achieved by the nonlinearity of a Boolean function. Thus, certainly one can efficiently use Boolean functions with high nonlinearity in coding theory and cryptography. For security reasons, the nonlinearity of Boolean functions must be high since the existence of affine approximations of the Boolean functions involved in a cryptosystem allows to build attacks on this system. In the case of stream ciphers, high nonlinearity is important to prevent fast correlation attacks and Linear Cryptanalysis for Block Ciphers [2,3,4].

Siegenthaler proposed the concept of correlation immunity in 1984. Correlation immunity is an interesting cryptographic property, which is to measure the level of resistance against correlation attacks. It is a safety measure for the correlation attack of nonlinear combiners. When used in a stream cipher as a combining function for linear feedback shift registers, a Boolean function with low-order correlation-immunity is more susceptible to a correlation attack than a function with correlation immunity of high order [4,5].

Algebraic immunity is a cryptographic property to measure the resistance against algebraic attack for stream ciphers. The concept of algebraic immunity of Boolean functions comes from the algebraic attack on stream ciphers proposed by Courtois and Meier in 2003 in [6], which has proven to be a very effective attack for both stream ciphers and block ciphers [4,7].

Zheng and Zhang in 1999 introduced plateaued Boolean functions for designing cryptographic functions as they have various cryptographic characteristics [8]. If squared Walsh transform of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ takes only one nonzero value then the function is known as plateaued [9]. Moreover, if the values of its Walsh transform belong to the set $\{0, \pm 2^{\frac{n+r}{2}}\}$ for some fixed r, $0 \leq r \leq n$ then the n-variable Boolean function is said to be r-plateaued. The cases of $r = 0, 1$ and 2 have attracted much attention due to their cryptographic algebraic and combinatorial properties [5].

Bent functions are 0-plateaued functions introduced by Rothaus in the year 1976 [10]. Bent functions are perfect nonlinear functions and have interesting implications to design block ciphers as well as stream ciphers. But these functions may not be compatible with other cryptographic design criteria as these functions cannot be implemented in conjunction with balance or highest nonlinear order [11]. Near bent functions are 1- plateaued functions on $\mathbb{F}_{2^n}$ exist only when n is odd and Semi bent functions are 2- plateaued functions on $\mathbb{F}_{2^n}$ exist only when n is even, introduced by Chee et al. in the year 1995 [12]. Similar to bent functions, semi bent functions and near bent functions are also widely

studied in sequences and cryptography. Unlike bent functions, semi bent functions and near bent functions are nearly perfect nonlinear so that they can be balanced and resilient. These functions are desirable for cryptographic applications as these functions have the low autocorrelation, a maximal nonlinearity among balanced plateaued functions, the high algebraic degree and satisfy the propagation criteria. They are also used for constructing the cryptographically robust S-blocks and widely used in code division multiple access (CDMA) communication systems for sequence design [5,13,14]. These semi bent and near bent functions are one of the most intensively studied topics related to bent functions.

Khoo et al. in 2002 gave the construction of n- variable quadratic semi bent functions in polynomial forms for both odd and even n [15]. Before his work, most of the researchers constructed semi bent function from power polynomials, that is, for suitably chosen d $f(x) = Tr(x^d)$. Dillon and McGuire in 2008 presented a general criterion for near bent functions to be bent on a hyperplane, and they showed that the Kasami-Welch function $Tr(x^d)$ is a bent function when restricted to the hyperplane of trace 0 elements in $\mathbb{F}_{2^n}$ [16]. Dong et al. in 2013 presented a new method for constructing semi bent function in polynomial form for both odd and even n with the help of few trace terms [17]. S. K. Pandey et al. presented an exhaustive construction of bent and balanced symmetric generalized functions (in form of ANF) on smaller domains [18].

From the above all observations, most of the researchers have focused on the construction of monomial semi bent and near bent functions. And few researchers have constructed these functions via composition and constructed in the polynomial form using few trace terms. To the best of our knowledge no work has been carried out so far to construct near bent function of the form $f(x) = (x^2+x)^d$ where d is Gold exponent (2^i+1) and we have also investigated some of the cryptographical properties as mentioned above. The improvement of cryptographic properties can be possibly expected with suitable modifications on the homomorphism functions similar to the functions used in [19].

2. Preliminaries

Definition of the near bent function is given by using Walsh-Hadamard coefficients.

Definition 2.1 ([9]). *The Walsh-Hadamard transform of a function f in n variables is the integer-valued function on $\mathbb{F}_2^n$, whose value at $a \in \mathbb{F}_2^n$ is defined as*

$$W_f(a) = \sum_{x \epsilon \mathbb{F}_2^n} (-1)^{f(x)+<a \cdot x>}.$$

As an example, one can use the usual inner product over $\mathbb{F}_2^n$, which is $a \cdot x = \sum_{i=1}^{n} a_i x_i \pmod 2$. If the vector space $\mathbb{F}_2^n$ is viewed as the structure of the

finite field $\mathbb{F}_{2^n}$, the usual inner product is nothing but $a \cdot x = tr_n(ax)$, where $tr_n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace function.

Definition 2.2 ([5]). *A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called a near bent if its Walsh transform satisfies:*

$$W_f(a) \in \{0, \pm 2^{\frac{n+1}{2}}\}, \text{ for all } a \in \mathbb{F}_{2^n}$$

Near bent functions on $\mathbb{F}_{2^n}$ exist only when n is odd.

Definition 2.3 ([20]). *The non-linearity of a Boolean function f is denoted by $nl(f)$ and is defined as*

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} W_f(a).$$

Definition 2.4 ([14]). *A sub function of order k of Boolean function f in variables $x_1, \ldots, x_n$ is a function $f^{i_1,\ldots,i_k}_{a_1,\ldots,a_k}$ where each variable x_{i_j} is fixed by the value a_{i_j}, $j = 1, \ldots, k$, $0 < k \leq n$.*

Definition 2.5 ([14]). *A Boolean function f in n variables is called correlation immune of order k if the weight of any of its sub function of order k equals $wt(f)/2^k$.*

Definition 2.6 ([14]). *The minimum algebraic degree of a Boolean function g, $g \neq 0$, such that $f \cdot g = 0$ or $(f \oplus 1) \cdot g = 0$ is called the algebraic immunity of f, and is denoted by AI(f).*

Definition 2.7 ([21]). *If c is an element of $K = GF(q^n)$, its trace relative to the subfield $F = GF(q)$ is defined as follows:*

$$Tr_F^K(c) = c + c^q + c^{q^2} + \ldots + c^{q^{n-1}}.$$

Theorem 2.8 ([21]). *For all α, $\beta \in K$ we have*

$$Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta).$$

3. Algebraic construction of near bent function

Theorem 3.1. *The function of the form*

$$f(x) = Tr(x^2 + x)^{(2^i+1)},$$

is a near bent function with $\gcd(i, n) = 1$.

Proof. $(x^2 + x)^{2^i+1} = x^{2*(2^i+1)} + x^{2*2^i} * x + x^2 * x^{2^i} + x^{2^i+1}$.

Note that in the finite field $\mathbb{F}_{2^n}$ holds $x^{2*(2^i)} = x^{2^i}$. Therefore, $(x^2+x)^{2^i+1} = x^{2^i+1}+x^{2^i}*x+x^2*x^{2^i}+x^{2^i+1} = x^{2^i+1}+x^{2^i+2}$. Walsh transform for the function $f(x) = Tr((x^2+x)^{2^i+1})$ is

$$W_f(a) = \sum_{x\epsilon\mathbb{F}_2^n} (-1)^{Tr(x^{2^i+1}+x^{2^i+2})\oplus<a\cdot x>} \tag{1}$$

Walsh transform for the function $f(x) = Tr((x)^{2^i+1})$ is

$$W_f(a) = \sum_{x\epsilon\mathbb{F}_2^n} (-1)^{Tr(x)^{2^i+1}\oplus<a\cdot x>} \tag{2}$$

Equation (1) has same terms as that of equation (2), except that the one term $Tr(x^{2^i+2})$ is extra. So we consider the following two cases regarding extra term.

Case 1. When $Tr(x^{2^i+2}) = 0$.

The term of the Boolean function will be $Tr((x)^{2^i+1})+0$, which is $Tr((x)^{2^i+1})$. Hence it is near bent function by [14].

Case 2. When $Tr(x^{2^i+2}) = 1$.

The terms of the Boolean function will be $Tr((x)^{2^i+1})+1$, whose values will be exactly opposite to that of equation (2). As $f(x) = Tr((x)^{2^i+1})$ is near bent function, the function $f(x) = Tr((x^2+x)^{2^i+1})$ is also near bent over $\mathbb{F}_2^n$.

Thus the function defined on $\mathbb{F}_2^n$ by

$$f(x) = Tr((x^2+x)^{2^i+1})$$

with $\gcd(i,n) = 1$ is a near bent over $\mathbb{F}_2^n$. □

If $\gcd(i,n) \neq 1$, then the functions $Tr((x^2+x)^{2^i+1})$ cannot be near bent function, which can be observed over some fields from the following examples.

Example 3.2. Over $\mathbb{F}_2^5$, the function $f(x) = Tr((x^2+x)^{2^5+1})$ is not a near bent function.

In fact, the values of Walsh transform $W_f(a)$ are 0 or -32, for all $a \epsilon \mathbb{F}_2^5$.

Hence $f(x) = Tr((x^2+x)^{33})$ is not a near bent function.

Example 3.3. Over $\mathbb{F}_2^9$, the function $f(x) = Tr((x^2+x)^{2^3+1})$ is not a near bent function.

In fact, the values of Walsh transform $W_f(a)$ are 0 or ± 64, for all $a \epsilon \mathbb{F}_2^9$.

Hence $f(x) = Tr((x^2+x)^9)$ is not a near bent function.

4. Cryptographic properties of above constructed near bent functions

There are many different kinds of attacks on the stream ciphers, and hence the Boolean functions used in the stream ciphers should have essential properties. Boolean functions play an important role in both error correcting coding activities and cryptography. Indeed, cryptographic transformations can be developed by the appropriate composition of nonlinear Boolean functions. Moreover, every code of length 2^n, for some nonnegative integer n, can be interpreted as a set of Boolean functions. In both frameworks, n is rarely large, in practice. The error correcting codes derived from n-variable Boolean functions have length 2^n; so, taking $n = 11$ already gives codes of length 2048. In the case of stream ciphers, n was in general at most equal to 11 until recently [4,5,14].

Moreover, Some of the important and very common cryptographic properties of near bent functions are briefly described in next sections.

4.1 Nonlinearity

The nonlinearity of the functions which are constructed using the theorems above is tabled for some values of i and n as follows.

Table 1: Nonlinearity of function $f(x) = Tr((x^2+x)^{2^i+1})$, with (i) $\gcd(i,n) = 1$ (ii) $\gcd(i,n) \neq 1$

(i)

i \ n	3	5	7	9	11
1	2	12	56	240	992
2	2	12	56	240	992
3		12	56		992
4	2	12	56	240	992
5	2		56	240	992

(ii)

i \ n	3	5	7	9	11
1					
2					
3	0			224	
4					
5		0			

The above Tables represent the nonlinearity values of the constructed near bent functions and Boolean functions for different values of i and n. For instance, for $i = 3$ and $n = 11$, the Table (1(i)) shows that nonlinearity of the function is 992. The same comparison is true for other values of i and n.

From the above Tables (1) and (1(ii)), it is clear that the nonlinearity of a newly constructed near bent functions in the Tables (1(i)) is more than that of Boolean functions in the Tables (1(ii)).

4.2 Correlation immunity

The below Tables (2(i), 2(ii)), represent the correlation immunity of the newly constructed near bent function and Boolean function. The correlation immunity

for the constructed near bent functions in Tables (2(i)) found to have the low number when compared to the Boolean function of the form in the Tables (2(ii)).

Table 2: Correlation Immunity of function $f(x) = Tr((x^2 + x)^{2^i+1})$, with (i) $\gcd(i, n) = 1$ (ii) $\gcd(i, n) \neq 1$.

(i)

i \ n	3	5	7	9	11
1	0	0	0	0	0
2	0	0	0	0	0
3		0	0		0
4	0	0	0	0	0
5	0		0	0	0

(ii)

i \ n	3	5	7	9	11
1					
2					
3	2			0	
4					
5		4			

4.3 Algebraic immunity

The below Tables (3(i),3(ii), represent the algebraic immunity values of the near bent functions and Boolean functions. The constructed near bent function exhibit more algebraic immunity, which can be observed by in Tables (3(i)) and (3(ii)). Further, it is worth noticing that the use of near bent functions will enhance the security of cryptosystems.

Table 3: Algebraic immunity of function $f(x) = Tr((x^2 + x)^{2^i+1})$, with (i) $\gcd(i, n) = 1$ (ii) $\gcd(i, n) \neq 1$.

(i)

i \ n	3	5	7	9	11
1	1	2	2	2	2
2	1	2	2	2	2
3		2	2		2
4	1	2	2	2	2
5	1		2	2	2

(ii)

i \ n	3	5	7	9	11
1					
2					
3	0			2	
4					
5		0			

5. Conclusion

The cryptographic properties nonlinearity, correlation immunity, and algebraic immunity are exhibited remarkably by near bent functions which are constructed using Gold power functions. The similar properties are expected to in case of large values of n too.

6. Acknowledgements

The corresponding author and the second author acknowledges Manipal Institute of Technology (MIT), Manipal Academy of Higher Education, India for their kind encouragement. The first author is grateful to Manipal Academy of Higher Education for their support through the Dr. T. M. A. Pai Ph. D. scholarship program.

References

[1] C. E. Shannon, *Communication theory of secrecy systems*, Bell System Technical Journal, 28 (1949), 656-715.

[2] W. Meier and O. Staffelbach, *Fast corrrelation attacks on stream ciphers*, Springer, Berlin, Heidelberg, 1988.

[3] C. Carlet, *Nonlinearity of boolean functions,* 848-849. Boston, MA, Springer US, 2011.

[4] C.-K. Wu and D. Feng, *Boolean functions and their applications in cryptography*, Springer-Verlag Berlin Heidelberg, 2016.

[5] S. Mesnager, *Bent functions*, Springer, 2016.

[6] N. T. Courtois and W. Meier, *Algebraic attacks on stream ciphers with linear feedback*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, 345-359.

[7] D. H. Lee, J. Kim, J. Hong, J. W. Han, and D. Moon, *Algebraic attacks on summation generators*, in International Workshop on Fast Software Encryption, Springer, 2004, 34-48.

[8] Y. Zheng and X.-M. Zhang, *Plateaued functions*, Springer Berlin Heidelberg, 1999, 284-300.

[9] C. Carlet, *Boolean and vectorial plateaued functions and apn functions,* IEEE Transactions on Information Theory, 61 (2015), 6272-6289.

[10] O. S. Rothaus, *On bent functions,* Journal of Combinatorial Theory, Series A, 20 (1976), 3 (1976), 300-305.

[11] W. Meier and O. Staffelbach, *Nonlinearity criteria for cryptographic functions,* Berlin, Heidelberg, Springer Berlin Heidelberg, 1990, 549-562.

[12] S. Chee, S. Lee, and K. Kim, *Semi-bent functions,* Berlin, Heidelberg, Springer Berlin Heidelberg, 1995, 105-118.

[13] K. Khoo, G. Gong, and D. R. Stinson, *A new characterization of semi-bent and bent functions on finite fields*, Designs, Codes and Cryptography, 38 (2006), 279-295.

[14] N. Tokareva, *Bent functions: results and applications to cryptography*, Academic Press, 2015.

[15] K. Khoo, G. Gong, and D. R. Stinson, *A new family of gold-like sequences,* in Information Theory, Proceedings, 2002 IEEE International Symposium, p. 181, IEEE, 2002.

[16] J. Dillon and G. McGuire, *Near bent functions on a hyperplane,* Finite Fields and Their Applications, 14 (2008), 715-720.

[17] D. Dong, L. Qu, S. Fu, and C. Li, *New constructions of semi-bent functions in polynomial forms,* Mathematical and Computer Modelling, 57 (2013), 1139-1147.

[18] S. K. Pandey, P. Mishra, and B. Dass, *Count and cryptographic properties of generalized symmetric boolean functions,* Italian journal of pure and applied Mathematics, 37 (2017), 173-182.

[19] S. P. Kuncham, B. Jagadeesha, and B. S. Kedukodi, *Interval valued l-fuzzy cosets of nearrings and isomorphism theorems,* Afrika Matematika, 27 (2016), 393-408, 2016.

[20] C. Carlet, *Open Questions on Nonlinearity and on APN Functions,* Cham: Springer International Publishing, 2015, 83-107.

[21] R. J. McEliece, *Finite fields for computer scientists and engineers*, Springer Science & Business Media, 2012, 23 (2012).

Accepted: 1.03.2019